1 Day Training Module
CDAC-MOHALI

# Web Application Security

## Module

- ✓ Introduction to Cyber Security
- ✓ Discussion on top threats and vulnerabilities
- ✓ Introduction to Proxy and Firewall servers
- ✓ Top 10 Web Application Attacks and its remedies – OWASP Top 10
- ✓ Foot printing and Information Gathering techniques (GHDB)
- ✓ Breaking into Databases – SQL Injection (String bases, Error based, Query based, Boolean based, Blind based etc)
- ✓ Input Validation Attacks
- ✓ Cross Site Scripting (Persistent, Non-Persistent, Dom Based)
- ✓ Remote and Local File inclusion (RFI and LFI)
- ✓ Cross site request forgery (CSRF) and Token Implementation
- ✓ Exploiting ASP DOT Net Based servers
- ✓ Shell Command line Injection
- ✓ Symlinking Attacks on Linux Servers
- ✓ Server Rooting (Windows and Linux based)
- ✓ CMS Foot printing and Exploitation
- ✓ Review on Exploits and Vulnerability Databases
- ✓ Creating Backdoors and its Identification
- ✓ DOS and DDOS Attacks – Prevention and Exploitation
- ✓ Apache and IIS Privilege Escalation
- ✓ Buffer overflow Exploitation
- ✓ Discussion on Complete Website & Server Security
- ✓ WordPress and Joomla Exploitation
- ✓ Discussion on Cyber Crime Laws
- ✓ Web application Security tools discussion
- ✓ Server Exploitation and its Security